THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

EDDIESTEALER

[Malware]

Description

EDDIESTEALER

CATEGORY

Malware

SEVERITY

High

Platforms

Windows

IMPACT

- Credential Theft
- System Reconnaissance
- Data Exfiltration to C2 Server

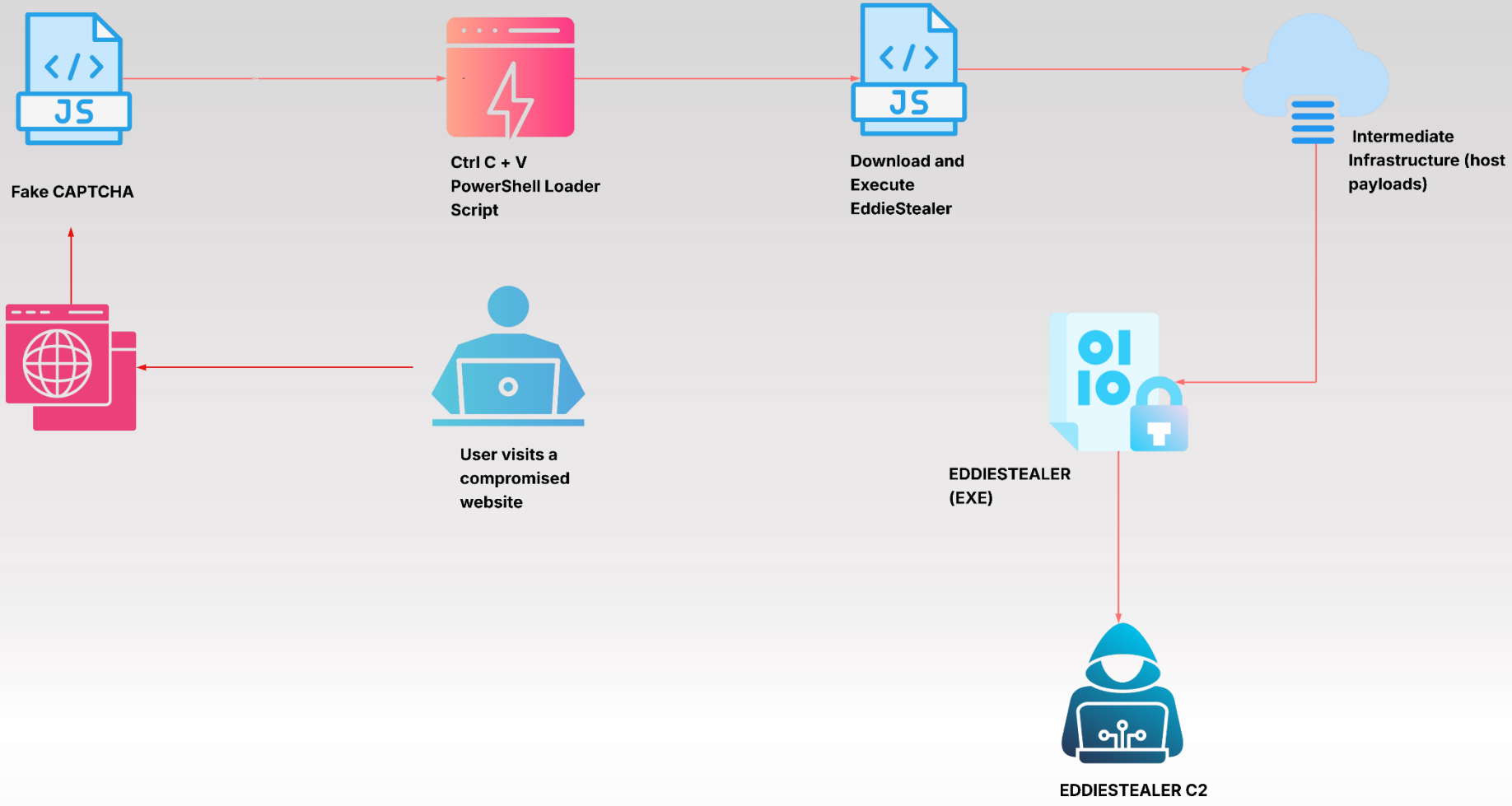
Threat actors are actively distributing a **new Rust-based information stealer dubbed *EDDIESTEALER*** using a deceptive social engineering method known as **ClickFix**, which initiates infection via **fake CAPTCHA verification pages** embedded into **compromised websites**.

Key Highlights:

- **Initial Vector:** Legitimate websites compromised to serve malicious JavaScript (gverify.js) posing as CAPTCHA validation.
- **Execution Method:** Victims are tricked into executing a **malicious PowerShell command** through Windows Run dialog.
- **Payload Delivery:** Obfuscated scripts download EDDIESTEALER binary from llll[.]fit, saved with randomized names in the Downloads directory.

Process Evaluation

EDDIESTEALER's execution chain



Indicator of Compromise

SHA-256

47409e09afa05fcc9c9eff2c08baca3084d923c8d82159005dbae2029e1959d0
162a8521f6156070b9a97b488ee902ac0c395714aba970a688d54305cb3e163f
f8b4e2ca107c4a91e180a17a845e1d7daac388bd1bb4708c222cda0eff793e7a
53f803179304e4fa957146507c9f936b38da21c2a3af4f9ea002a7f35f5bc23d
20eeae4222ff11e306fded294bebea7d3e5c5c2d8c5724792abf56997f30aaf9
1bdc2455f32d740502e001fce51dbf2494c00f4dcadd772ea551ed231c35b9a2
d905ceb30816788de5ad6fa4fe108a202182dd579075c6c95b0fb26ed5520daa
b8b379ba5aff7e4ef2838517930bf20d83a1cfec5f7b284f9ee783518cb989a7
f6536045ab63849c57859bbff9e6615180055c268b89c613dfed2db1f1a370f2
d318a70d7f4158e3fe5f38f23a241787359c55d352cb4b26a4bd007fd44d5b80
73b9259fecc2a4d0eeb0afef4f542642c26af46aa8f0ce2552241ee5507ec37f
2bef71355b37c4d9cd976e0c6450bfed5f62d8ab2cf096a4f3b77f6c0cb77a3b
218ec38e8d749ae7a6d53e0d4d58e3acf459687c7a34f5697908aec6a2d7274d
5330cf6a8f4f297b9726f37f47cffac38070560cbac37a8e561e00c19e995f42
acae8a4d92d24b7e7cb20c0c13fd07c8ab6ed8c5f9969504a905287df1af179b
0f5717b98e2b44964c4a5dfec4126fc35f5504f7f8dec386c0e0b0229e3482e7
e8942805238f1ead8304cfdcf3d6076fa0cdf57533a5fae36380074a90d642e4
7930d6469461af84d3c47c8e40b3d6d33f169283df42d2f58206f43d42d4c9f4

MD5

5a75e2be32ccb29cbe4cc193e26ec9bc
673c99885c030506fff25f1c23ae06b8
02c100acfedebccc676f9b8af8e7e2b5
0e9b5fda2deb50e26ab23abd294286c5
ec45ccb0b9114b304f76b8c0eb1c79bc
c6857063b678f8b539ac9525fd3c7e0b
c21c7aac8d0c9e72a45f2cef7a5f6455
20745dc4d048f67e0b62aca33be80283
6cc654225172ef70a189788746cbb445
c8c3e658881593d798da07a1b80f250c
4776ff459c881a5b876da396f7324c64
6342c05504154d958af852b3ea265afc
64d3d33cba202938a01ee2af728a5813
cf2915ed4e234456ad687696231821c3
9e4cf859827498070f8709b047d0430d
a034dbfd78b95e121d7603626f19f2a7
23def2d18b9dd3cd4edcfe9e9b7901cf
d2787deb38273a8172e3180e884dc6ad

IPs

45.144.53.145
84.200.154.47

Domains

shiglimugli.xyz
xxxivi.com
llll.fit
plasetplastik.com
militrex.wiki

SHA-1

43c067d626bd87692f33714760825f3d37c1f1c5
13a8b21cd959d5b986a28bcee76bd49b183d50f7
7ae1bda95748354597fdd107d245ecc088b57f76
264c4c5b8f0edfa53e95eb46fa081ccf9cc01469
ec29ce94832ca4367922bcfc9c0b829dde1da584
6c1a3b6334db20cdcecbca4aead2d0ae707fac79
129aea3bc9494700d5d2cd887a64ff5588c4bcbf
e8f9ac7ca019c83590cb7d9302d1d24ad2a27010
b00652396d2c5ae770a1762fe0c06c2de6d10b9c
34868b61cb7e395c9ab1e9f449bc921ec8ee6d46
af906519b48867d9f9e75f9ca9951995ef53b57f
e2ac7fd1a4326b3e033b8153f0506e57837172fe
9e06155f24320783be182d70b0c61f8574605424
a752a17d96cc3372bfa5e4b15821a7feb5e3e3b4
bf023c7705bedd0401f95e110701435167007703
76efb9cc79576417e97ee5895b5c33dc590df2a5
b0079cf3732b068166b373c51386986420efa765
75ca207683313392e4ef3cad23b83b5ed7c476e8

Remediation

1. User Awareness

- Conduct security awareness training for users to recognize suspicious websites, LNK shortcuts, and unexpected ZIP attachments.
- Block known EDDIESTEALER-related IPs, URLs, and download domains at the network perimeter.

2.. Incident Response Readiness

- Test your organization’s detection and containment capabilities via tabletop exercises involving APT-level threats.
- Establish IOCs (Indicators of Compromise) in EDR/SIEM systems for early warning and blocking.

ThreatCure

Cyber Threat Advisory

Secure your byte world

EDDIESTEALER

[Malware]